CLAIMS

1. A method of performing a service for a requestor on a computing platform, comprising:

the requestor providing a specification of the service to be performed to the computing platform, wherein the specification of the service establishes specified levels of trust for at least some of the processes in the service;

the computing platform executing the service according to the specification and logging performance of at least some of the processes for which a level of trust was specified; and

the computing platform providing the requestor with a log of the performance of the processes performed according to the specified levels of trust.

2. A method as claimed in claim 1, wherein no performance logging takes place for at least some of the processes for which a level of trust is specified in the specification.

3. A method as claimed in claim 1, wherein the computing platform contains a physically and logically protected computing environment.

4. A method as claimed in claim 3, wherein said physically and logically protected computing environment contains a monitoring process for measuring integrity of the computing platform.

5. A method as claimed in claim 3, wherein a service management process allocates the execution of processes and logging of performance to discrete computing environments in or associated with the computing platform.

6. A method as claimed in claim 5, wherein the service management process is located within the protected computing environment.

7. A method as claimed in claim 5, wherein one or more of the discrete computing environments is a compartment containing a computing engine protected against influence from outside the compartment by operational or environmental constraints.

8. A method as claimed in claim 7, wherein the computing engine is a Java virtual machine.

9. A method as claimed in claim 7, wherein one or more compartments is located within the protected computing environment.

10. A method as claimed in claim 7, wherein the computing engine is constrained not to operate on input data if it is not permitted to do so.

11. A method as claimed in claim 10, wherein input data is provided with a data type, and a process is provided with operation types, and operation is prevented if operation types and data types are not consistent.

12. A method as claimed in claim 10, wherein input data may have an owner, and the process may be required to inform the owner of use of the input data.

13. A method as claimed in claim 10, wherein input data may have an owner, and if so, the process may be required to obtain consent from the owner to use of the input data.

14. A method as claimed in claim 5, wherein a process may be swapped between one discrete environment and another discrete environment.

15. A method as claimed in claim 1, wherein performance logging includes logging of input data to a process.

16. A method as claimed in claim 1, wherein performance logging includes logging of output data from a process.

17. A method as claimed in claim 1, wherein performance logging includes logging of program instructions executed in performance of a process.

18. A method as claimed in claim 1, wherein data logged is sampled according to a sampling process to provide the performance log.

19. A method as claimed in claim 18, wherein the sampling process is performed according to a function to provide irregular sampling.

20. A method as claimed in claim 1, where a digest of data logged is obtained as part of the performance logging data.

21. A method as claimed in claim 1, wherein the performance logging data is encrypted before it is sent to the requestor.

22. A method as claimed in claim 1, wherein the specification establishes performance logging parameters for at least some of the processes in the service.

23. A method as claimed in claim 4, wherein the monitoring process provides an integrity metric of the computing platform to the requestor current when the service was performed.

24. A computing platform, comprising:

a physically and logically protected computing environment, adapted to provide trustworthy data to appropriate users of the computing platform; and

one or more compartments, arranged to operate in a sufficiently constrained manner that processes executed in a compartment are performed reliably;

wherein specified processes may be executed for a user in the one or more compartments and the results of the specified processes returned to the user in trustworthy data from the protected computing environment.

25. A computing platform as claimed in claim 24, wherein one or more of said compartments are located outside the protected computing environment.

26. A computing platform as claimed in claim 24, wherein one or more of said compartments are located inside the protected computing environment.

27. A computing platform as claimed in claim 24, wherein each compartment contains a virtual computing engine.

28. A computing platform as claimed in claim 27, wherein the virtual computing engine is a Java virtual machine.

29. A computing platform as claimed in claim 24, wherein the protected computing environment contains a monitoring process adapted to measure the integrity of the computing platform.

30. A computing platform as claimed in claim 24, wherein the computing platform contains a service management process adapted to receive a service description which includes levels of trust assigned to processes within the service, and to allocate at least some of the processes to the compartments.

31. A computing platform as claimed in claim 30, wherein service management process is located within the protected computing environment.